BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 80 du 21 octobre 2022

TEXTE RÉGLEMENTAIRE PERMANENT

Texte 16

INSTRUCTION ARM/CAB

fixant la gouvernance ministérielle du numérique et des systèmes d'information et de communication (SIC).

Du *09 septembre 2022*

DIRECTION GÉNÉRALE DU NUMÉRIQUE ET DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION :

INSTRUCTION ARM/CAB fixant la gouvernance ministérielle du numérique et des systèmes d'information et de communication (SIC).

Du 09 septembre 2022

NOR A R M D 2 2 0 2 3 9 9 J

Référence(s) :
Voir annexe 1.

Pièce(s) jointe(s) :
Quatre annexes.

Classement dans l'édition méthodique :
BOEM 160.1.1.

Référence de publication :

SOMMAIRE

Préambule

Le décret de référence 1) fixe l'organisation du système d'information et de communication de la défense et porte création de la direction générale du numérique et des systèmes d'information et de communication. L'arrêté de référence 7) porte création et organisation d'instances relatives au système d'information et de communication de la défense. Ces textes instituent le dispositif de gouvernance numérique ministérielle, qui permet d'élaborer collégialement les principales décisions et d'en suivre la mise en œuvre. La présente instruction vise à définir les modalités particulières de mise en œuvre de cette gouvernance numérique ministérielle et en particulier les rôles, les responsabilités et les instances associées. Elle précise enfin l'articulation avec la gouvernance capacitaire, ainsi que la répartition des responsabilités dans l'examen des projets et systèmes.

1. OBJET ET DOMAINE D'APPLICATION

Cette instruction s'applique au système d'information et de communication de la défense, défini à l'article 1 du décret de référence 1)[1].

Elle vient en complément des instructions relatives aux opérations d'investissement du ministère des armées (cf. référence 13), passages en CMI[2]), à la maîtrise des risques et au contrôle interne budgétaire (cf. référence 17), examen en CEI[3]).

Les attributions de la DGNUM prévues par l'article 11 du décret de référence 1) relatives à la sécurité du numérique, sont exercées au sein d'instances de gouvernance de la sécurité du numérique sous l'égide de la DPID[4]. Elles sont donc exclues du périmètre de la présente instruction.

2. RÔLES ET RESPONSABILITÉS DE GOUVERNANCE

Une représentation des relations entre les acteurs présentés dans le présent chapitre est proposée en annexe 3.

2.1. **Le responsable de segment**

Le chef d'état-major des armées (CEMA), le délégué général pour l'armement (DGA) et le secrétaire général pour l'administration (SGA), sont respectivement responsables des segments SIOC[5], SIST[5] et SIAG[5], définis dans l'arrêté de référence 7).

2.2. **L'autorité de domaine**

Un domaine désigne un ou plusieurs métiers corrélés, relevant d'une même autorité organique, l'autorité de domaine.

Dix-sept domaines sont identifiés :

- Périmètre CEMA : Armée de Terre - préparation des forces, MCO Terrestre, Marine - préparation des forces, MCO Naval, Armée de l'Air et de l'Espace - préparation des forces, MCO Aéronautique, Commandement et Contrôle et Interarmées (C2&IA), Renseignement, Appui SIC, Soutien Commissariat des armées, Soutien Santé ;
- Périmètre DGA : Systèmes numériques de l'armement ;
- Périmètre SGA : Ressources Humaines, Immobilier, Finances Achats, Transverse ;
- Périmètre DRSD : Renseignement de sécurité et de défense.

L'autorité de domaine (AdD) est responsable des arbitrages et des priorisations sur les enjeux et les objectifs de réalisation et de performance SIC de son domaine, afin de répondre aux attentes et besoins exprimés. Dans ce cadre, elle s'appuie sur une DSI[6] Domaine qui lui est subordonnée.

L'AdD confie à la DSI précitée la gestion et le pilotage d'un portefeuille projets et SI ; cette dernière a la charge d'étudier, de concevoir, de réaliser, de maintenir et d'exploiter les projets et SI de son portefeuille.

La DSI Domaine, en liaison avec le directeur de données ou ses délégués, propose à l'AdD, pour validation et signature, un schéma directeur « SI et données » mis à jour périodiquement (cible annuelle). Dans le cadre fixé par la politique ministérielle, ce document prend en compte le ou les schémas directeurs définis par le ou les RZF[7] (et/ou RQF[7]) et les travaux de la chaine capacitaire pour les opérations d'armement.

Dans le respect des responsabilités dévolues au(x) RZF, en lien avec la DSI Domaine, l'AdD assure les cohérences fonctionnelle, technique et métier et la maîtrise du coût global de possession (MCO/MCS compris) des SI du domaine.

2.3. **L'autorité cliente**

L'autorité cliente (AC) est l'autorité responsable de l'activité métier. Elle définit pour le compte des autorités utilisatrices le besoin fonctionnel, le périmètre du projet et sa date de mise en service opérationnel (MSO) souhaitée. Conformément aux échanges avec les utilisateurs, elle définit de manière globale, les conditions de mise en œuvre du SI et les objectifs de sécurité (modes de travail, processus, articulation avec d'autres métiers…).

L'AC est responsable de porter le projet devant la gouvernance, en présentant le projet considéré au responsable de segment, qui est chargé de prononcer le changement des phases (préparation, réalisation et utilisation) décrites dans l'instruction de référence 16), conformément aux dispositions du paragraphe 4.2 – *infra*. Elle bénéficie du soutien du (ou des) RZF concerné(s), ainsi que du (ou des) directeur(s) des données concerné(s).

Dès la phase de préparation, l'AC exprime le besoin et désigne un responsable fonctionnel (RF) qui relève de son autorité, et qui portera le besoin pendant toute la vie du SI jusqu'à son retrait de service. Lorsqu'il y a plusieurs autorités utilisatrices, l'AC doit prendre en compte leurs besoins et échanger régulièrement avec elles sur le SI et les évolutions envisagées.

Un responsable de conduite de projet (RCP) est désigné sous couvert de l'autorité de domaine et en accord avec la DSI concernée.

L'AC préside le comité directeur (CODIR) du projet (hors opération d'armement), auquel elle associe notamment le responsable de segment, le (ou les) RZF concerné(s) et les autorités utilisatrices.

2.4. **La DSI Groupe**

La DGNUM[8] assure le rôle de DSI Groupe.

Dans le cadre de la politique ministérielle du numérique, la DSI Groupe assure les principales missions suivantes en veillant à la prise en compte équilibrée des enjeux particuliers relatifs à la sécurité du numérique :

- elle propose les orientations stratégiques et la politique ministérielle dans le domaine du numérique et des SIC en concertation avec les trois grands subordonnés, contrôle leur mise en œuvre et assure la cohérence d'ensemble du système d'information et de communication de la défense ;
- elle s'assure de la maitrise du patrimoine applicatif et du portefeuille projets par les DSI Domaines, DSI Socle et Cyber ; cette cartographie inclut les informations relatives à la sécurité du numérique (incluant la défendabilité) définies en coordination avec la DPID, le COMCYBER[9] et les AQSSI[10] ;
- en cas d'incompatibilité potentielle avec la politique numérique ministérielle, la DSI Groupe soumet à l'arbitrage de la gouvernance numérique les décisions de lancement ou d'évolution majeure de systèmes d'information ;
- les projets et évolutions majeures de systèmes d'information et de communication répondant à des caractéristiques de coût prévisionnel ou présentant un fort enjeu ministériel lui sont soumis pour avis conforme dans les conditions précisées par arrêté (cf. référence 3) ;
- les projets relevant du périmètre du SI de l'État et répondant à des caractéristiques, notamment de coût prévisionnel, fixées par arrêté du Premier ministre (cf. référence 4), sont soumis via la DSI Groupe pour avis conforme au directeur interministériel du numérique ;
- au titre de l'architecture d'entreprise[11] et en concertation avec l'ensemble des acteurs du numérique, elle définit les dispositions d'architecture générale, le cadre de cohérence du système d'information et de communication de la défense ; elle assure la gouvernance des référentiels fonctionnel, applicatif, technique et donnée, crée et entretient la cartographie associée à ces différents axes. Elle en contrôle la mise en œuvre. Elle vise les schémas directeurs SI et données préparés par les DSI Domaines en s'assurant de leur cohérence ;
- en matière budgétaire, elle participe aux travaux de planification et de programmation militaire sur l'ensemble du domaine du numérique et des systèmes d'information et de communication. À ce titre, elle porte la programmation pluriannuelle des dépenses relatives au socle numérique ministériel mutualisé ;
- elle contribue à la gestion prévisionnelle des ressources humaines conduite au niveau ministériel et relative aux compétences nécessaires à la mise en œuvre et à la sécurité du système d'information et de communication de la défense. Elle propose aux organismes gestionnaires ou employeurs de la famille

professionnelle « systèmes d'information et de communication » la mise en œuvre de toute mesure relevant de leur compétence et de nature à favoriser cette gestion prévisionnelle ;

- elle conçoit et coordonne les évolutions structurantes indispensables à la transformation numérique du ministère ; elle s'assure de l'adéquation entre la trajectoire du socle numérique ministériel mutualisé portée par la DSI Socle et la DSI Cyber et les besoins applicatifs portés par les DSI Domaines ;
- elle anime la communauté des acteurs ministériels du numérique, elle veille à leur bonne information sur le référentiel applicable et les objectifs stratégiques ; elle contribue au rayonnement de la politique ministérielle, en interne comme en externe, sans préjudice des prérogatives des grands subordonnés ;
- en concertation avec la DPID, elle veille à la prise en compte des objectifs de sécurité du numérique au sein de l'architecture générale des systèmes d'information du ministère ; elle s'assure que les obsolescences majeures font l'objet d'actions concrètes de la part des DSI afin de limiter les risques de sécurité du numérique ; elle s'assure de la prise en compte de la conformité au droit du numérique ; elle s'assure de la bonne intégration de la sécurité du numérique dans les projets numériques à chaque étape de leur cycle de vie, de la conception au retrait de service ;
- en tant qu'administrateur ministériel des données, des algorithmes et des codes sources (AMDAC), et en concertation avec l'ensemble des acteurs de la gouvernance des données, elle définit la politique ministérielle d'ouverture et de valorisation des données ;
- elle assiste et conseille les DSI Domaines, Socle et Cyber. Chaque DSI relève d'une AQSSI ;
- elle appuie le FSSI[12] pour l'évaluation des impacts sur le SI ministériel, induits par les évolutions de politiques, règlements, orientations en matière de sécurité du numérique.
- elle consulte la DPID sur tout document structurant de niveau ministériel afin de s'assurer que la sécurité du numérique est prise en compte.

2.5. **La DSI Cyber**

Pour contribuer à la sécurité du SI du ministère, la DSI Cyber assure un rôle de prescription en matière d'outils Cyber sur le socle auprès de la DSI Socle, mais aussi au profit des autres DSI du ministère et de l'agence du numérique de défense. Dans ce cadre, elle contribue aux travaux relatifs au cadre de cohérence technique (CCT). Par ailleurs, la DSI Cyber assure (à l'instar d'une DSI Domaine) la gestion de son portefeuille sur son périmètre.

2.6. **La DSI Socle**

Le socle numérique[13], bien commun ministériel (réseaux, postes de travail, data center, services collaboratifs…) constitue un domaine particulier, confié à la DIRISI[14] en tant que maîtrise d'ouvrage (MOA) intégrant une DSI Socle.

Garante de la cohérence d'ensemble des briques du socle numérique, la DSI Socle est responsable du pilotage de la feuille de route de la phase de définition à l'exploitation courante. Elle contribue à l'instruction des travaux du COF[15] en analysant les demandes d'évolution et les besoins nouveaux du socle exprimés par les DSI Domaines. La DSI Socle pilote la mise en production et en exploitation des différentes briques du socle. Par ailleurs, elle organise et suit la maintenance, l'amélioration continue et l'évolution des services. Elle pilote les travaux de gestion des données du socle. L'AND (agence du numérique de défense) agit en tant que maîtrise d'ouvrage déléguée. Ainsi, une DSI Domaine s'appuie sur les services et composants communs du socle numérique et sur l'infrastructure du ministère, mis à disposition par l'opérateur DIRISI. À ce titre, une DSI Domaine est un des clients du Socle. Elle définit et priorise, en lien avec son autorité de domaine, ses besoins en services du socle, nécessaires à ses missions, conformément aux besoins du métier qu'elle représente.

2.7. **La DSI Domaine**

Une DSI Domaine est une structure optimisée, subordonnée à une autorité de domaine, qui s'appuie sur les structures existantes de son écosystème.

La DSI Domaine intervient dans le cadre de la politique ministérielle relative au système d'information et de communication de la défense (cf. référence 1), dont la DSI Groupe assure la cohérence d'ensemble. À ce titre, la DSI Domaine veille au respect de l'ensemble des cadres ministériels.

Responsable du respect du coût global de possession, des délais, et de la performance des SI de son portefeuille, proche des utilisateurs, elle assure une mission de conseil et d'appui au commandement ainsi que la réalisation et le suivi de projets qui lui sont confiés comme maîtrise d'ouvrage déléguée.

Tête de chaîne SIC de son domaine (RSIC[16]), elle est responsable de la mise à disposition des produits et services numériques répondant aux besoins exprimés. Elle définit et priorise, en lien avec son autorité de domaine, ses besoins en services du socle, nécessaires à ses missions, conformément aux besoins du métier qu'elle représente.

Elle assure la gestion et le pilotage du portefeuille projets et SI qui lui a été confié par son autorité de domaine. Elle assure la programmation du budget des projets de son portefeuille en concertation avec le responsable de zone fonctionnelle concerné, ainsi que le suivi de l'exécution financière des SIC qui le composent.

Elle est responsable de la mise en œuvre de la politique des données du domaine (pilotage, architecture des données).

D'une manière générale, elle contribue à la rationalisation et à l'efficience du SI ; elle assure la cohérence d'ensemble de son portefeuille (notamment calendaire) et l'urbanisation au profit de son domaine. Elle maîtrise en permanence le portefeuille de projets, de produits et de services numériques qui lui a été confié.

Elle veille à la prise en compte permanente des différents aspects de sécurité du numérique de son portefeuille (cohérence, architecture d'ensemble) conformément à la politique ministérielle (cf. référence 10), en lien notamment avec l'autorité d'homologation dont dépendent les projets et SIC en service de son portefeuille notamment, et de cohérence fonctionnelle en lien avec le responsable de zone fonctionnelle (RZF). Elle assure le pilotage des actions de maîtrise des risques cyber de son portefeuille et décline les besoins stratégiques en matière de sécurité du numérique en identifiant les besoins de sécurité transverses. Elle assure également la conformité juridique et réglementaire des projets et SI de son portefeuille. Elle fait également respecter les prescriptions dans les domaines de la protection des données.

Elle veille à la prise en compte des directives et bonnes pratiques relatives aux clauses de sécurité des systèmes d'information à intégrer dans les marchés. Elle s'assure que les clauses (contrat, conventions, protocoles, etc.) relatives à la propriété intellectuelle contribuent aux objectifs du métier en matière de partage et ouverture maîtrisés de données, transparence des algorithmes et réutilisation des composants de SI (utilisés ou produits).

Elle est tête de chaîne pour la transformation numérique de son domaine.

Elle assure le suivi de ses compétences SIC.

Elle adopte une démarche numérique responsable (RSE[17]).

Elle capte, coordonne et soutient l'innovation numérique en lien avec son domaine en relation avec les entités en charge de l'innovation au sein du ministère.

2.8. **Le responsable de zone fonctionnelle (RZF)**

Le responsable de zone fonctionnelle (RZF) et le responsable de quartier fonctionnel (RQF) sont chargés d'assurer la cohérence de leur zone (ou quartier) en matière d'urbanisation.

Le RZF (ou le RQF) rédige et entretient le schéma directeur de sa zone (ou quartier). Il est responsable de l'optimisation des processus et du nombre d'applications, ainsi que responsable de la gouvernance de la qualité des données de sa ZF (ou QF), en liaison avec les autorités clientes et les autorités de domaine.

Il se prononce sur l'opportunité de lancer ou non le projet lors de la phase de préparation, sur les interfaces avec les SI des autres zones (ou quartiers), ainsi que sur le retrait de service des applications.

2.9. **L'agence du numérique de défense**

Conformément aux textes de références 5) et 20), l'agence du numérique de défense est notamment chargée :

- de conduire, pour le compte des états-majors, directions et services et tout au long de leur cycle de vie, les projets numériques dont la responsabilité lui est confiée ;
- de conseiller, au titre de la conduite des projets qu'elle assure, les états-majors, directions et services sur la définition de leurs besoins numériques et l'optimisation des ressources humaines et financières qu'ils leur consacrent ;
- de mettre en œuvre la politique industrielle du ministère de la défense dans le domaine des technologies numériques des systèmes d'information, en lien avec la direction générale du numérique et des systèmes d'information et de communication et le service des affaires industrielles et de l'intelligence économique de la direction générale de l'armement.

La conduite des projets complexes ou à fort enjeu a vocation à être confiée à l'AND. Conformément à l'arrêté de référence 5), le comité d'orientation et de pilotage (COP) de l'AND est notamment chargé d'arrêter, sur proposition du DGNUM établie en concertation avec le chef d'état-major des armées, le délégué général pour l'armement et le secrétaire général pour l'administration, la liste des projets dont la conduite est confiée à l'agence. Il soumet cette liste à l'approbation du ministre de la défense.

3. INSTANCES DE GOUVERNANCE

La gouvernance haute de l'ensemble des systèmes d'information et de communication de défense, garantissant une plus grande transversalité, est unifiée, en associant les grands subordonnés sous l'égide du conseil du numérique et des systèmes d'information et de communication[18] présidé par le ministre, et dont le secrétariat est assuré par le comité exécutif du conseil du numérique et des systèmes d'information et de communication (CECNUM), présidé par le DGNUM.

Les attributions de la DGNUM prévues par l'article 9 du décret de référence 1) relatives aux ressources humaines, sont exercées au sein d'instances de gouvernance des ressources humaines décrites par l'instruction ministérielle de référence 12). Elles ne sont donc pas présentées dans le présent chapitre.

3.1. **Les instances de gouvernance générale**

3.1.1. La gouvernance des segments

Les segments et instances de gouvernance associées sont définis dans l'article 5 du texte de référence 7).

Ces instances examinent et approuvent les projets et SIC en production des états-majors, direction et services selon les modalités qu'il leur convient de définir.

Pour le segment considéré, chaque commission met en place les instances qu'elle juge nécessaires et auxquelles elle peut déléguer sa responsabilité selon un principe de subsidiarité, tout en veillant à la bonne prise en compte des objectifs transversaux de la politique numérique ministérielle.

À ce titre, pour les SIAG et les SIOC, ces instances conduisent ou font conduire par subsidiarité, selon des modalités définies par instruction, les activités suivantes :

- adoption d'un schéma directeur pour les systèmes d'information de leur compétence. Ces schémas directeurs comprennent un volet stratégique déclinant le document de politique générale et un volet opérationnel constitué notamment de plans d'actions par domaines métiers ;
- établissement annuel d'un plan d'investissement couvrant les projets et activités de leur responsabilité en matière de systèmes d'information et de communication et de transformation numérique, et suivi de son exécution ;
- réalisation d'une revue annuelle des projets et produits, hors opération d'armement, en préparation, réalisation ou utilisation. Elles se prononcent sur le respect des dispositions d'architecture générale et du cadre de cohérence définis par la direction générale du numérique et des systèmes d'information et de communication, ainsi que sur leur programmation financière en tenant compte des priorités fixées par les états-majors, directions et services ;
- adoption annuelle de la liste des projets à fort enjeu ministériel et identification des projets susceptibles de faire l'objet d'un avis conforme au titre de l'article 5. du décret n° 2018-532 du 28 juin 2018 (référence 1) et de l'article 3. du décret n° 2019-1088 du 25 octobre 2019 (référence 2) ;
- examen et approbation des changements de phases et des franchissements de jalons, sur l'ensemble du cycle de vie, des projets présentés par les états-majors, directions et services.

Pour les SIST, la commission des systèmes d'expertise, essais et expérimentations porte sur un périmètre couvrant les systèmes en support des expertises, essais, et expérimentations techniques, technico-opérationnelles ou opérationnelles liés aux systèmes d'armes, aux systèmes d'information opérationnels et de communication, à leur mise en œuvre coordonnée.

À ce titre, la commission des systèmes d'expertise, essais et expérimentations conduit ou fait conduire par subsidiarité, selon des modalités définies par instruction, les activités suivantes :

- adoption d'un schéma directeur pour les systèmes d'information du périmètre de la commission ;
- adoption annuelle de la liste des projets à fort enjeu ministériel et identification des projets susceptibles de faire l'objet d'un avis conforme au titre de l'article 5. du décret n° 2018-532 du 28 juin 2018 (référence1) et de l'article 3. du décret n° 2019-1088 du 25 octobre 2019 (référence 2) ;
- examen des changements de phase et des franchissements de jalon des projets présentés par les états-majors, directions et services.

Pour prendre en compte dans l'exercice et la gouvernance des projets relatifs aux systèmes d'information logistiques (SIL) la bonne intégration des processus d'administration et de gestion qu'ils portent relevant de la responsabilité du SGA, un comité de cohérence et de gouvernance des SIL (COGESIL) dédié est réuni au moins une fois par an.

3.1.2. La gouvernance du socle numérique ministériel mutualisé

Le socle numérique ministériel mutualisé est conçu et opéré au bénéfice des trois segments. Le périmètre du socle numérique ministériel mutualisé est défini dans l'article 5 du texte de référence 7).

Maître d'ouvrage et opérateur du socle numérique ministériel mutualisé, la direction interarmées des réseaux d'infrastructure et des systèmes d'information de la Défense fournit les services du socle nécessaires à l'exercice des missions du chef d'état-major des armées, du délégué général pour l'armement et du secrétaire général pour l'administration ainsi que de l'ensemble des organismes de la Défense.

La cohérence d'ensemble du système d'information et de communication de la défense, notamment entre les systèmes d'information des trois segments et le socle numérique ministériel mutualisé, est assurée par le directeur général du numérique et des systèmes d'information et de communication.

Le socle numérique ministériel mutualisé relève des dispositions de gouvernance particulières précisées ci-dessous.

3.1.2.1. Orientations stratégiques

La gouvernance du socle s'appuie sur le comité d'orientation fonctionnel (COF), présidé par le directeur général du numérique et des systèmes d'information et de communication pour l'exercice de ses attributions de responsable de la cohérence d'ensemble entre les systèmes d'information des trois segments et le socle numérique.

Le COF se réunit deux fois par an. Le COF comprend des représentants des membres du comité exécutif ministériel du numérique et des systèmes d'information et de communication et les responsables des états-majors, directions ou services.

Le COF s'appuie sur les travaux de son secrétariat permanent du COF (SP COF). Le SP COF est animé par la DSI Groupe et est chargé d'instruire l'ensemble des tâches qui seront présentées au COF pour orientation. Il peut être saisi par tout acteur du numérique.

Le Comité d'orientation fonctionnel (COF) a pour missions de :

- examiner les besoins d'évolutions structurantes du socle technique et des services associés, préalablement priorisés par les grands subordonnés et recueillis par la DIRISI en tant que maîtrise d'ouvrage du socle ;
- faire mener de manière incrémentielle les analyses fonctionnelles et de la valeur pour les besoins d'évolutions structurantes ;
- valider les priorités des besoins retenus. En conséquence, valider les évolutions structurantes des feuilles de route des projets et opérations d'armement du socle (classifié et non classifié), au regard des besoins exprimés, de leurs impacts sur les systèmes d'information en exploitation ou en développement, des ressources financières et des ressources humaines et techniques des entités en charge de sa construction (principalement l'AND), de la DIRISI et des organismes en charge de l'exploitation fonctionnelle des services communs ;
- faire mener les analyses d'impacts des besoins en projet de socle sur les services en exploitation ou en cours de développement, au titre de la démarche d'architecture d'entreprise d'ensemble ;
- s'assurer de l'avancée de la satisfaction des besoins et du déploiement des composants du socle ;
- valider le plan d'équipement bureautique ministériel annuel élaboré par la DIRISI, constitué des nouveaux besoins et du renouvellement des postes de bureautique courante.

En charge du plan d'investissement SIC ministériel, la DGNUM assure la cohérence générale d'ensemble des priorités fixées par le COF sur le socle numérique en lien avec les plans d'investissement des programmes 178, 146 et 212.

En outre, le COF s'assure de la prise en compte des orientations du COMCYBER en matière de défendabilité des composants du socle et d'intégration des produits de sécurité associés au socle.

3.1.2.2. Pilotage

Le socle est articulé par la DIRISI, en tant que maîtrise d'ouvrage, en blocs cohérents de projets et produits, chacun de ces blocs étant supervisé par un comité de pilotage chargé d'orienter les projets et les évolutions des produits, de prendre les décisions de son niveau et de contrôler l'action des équipes.

Ces comités de pilotage sont présidés par la DIRISI, appuyée par l'agence du numérique de défense en tant que maitrise d'ouvrage déléguée. Les responsables de segment et le directeur général du numérique et des systèmes d'information et de communication sont membres de droit de ces comités de pilotage.

Ces comités de pilotage veillent plus particulièrement à :

- prendre en compte les besoins formulés et priorisés par les segments vis-à-vis du socle numérique ministériel mutualisé ;
- examiner et instruire les besoins d'évolutions du socle technique et des services associés qu'ils ne jugent pas structurantes ;
- l'avancement des feuilles de route conformément aux priorités et orientations du COF ;
- la coordination technique et calendaire avec les projets et produits des segments.

Concernant la définition de l'environnement numérique de travail commun au ministère, le comité de pilotage est coprésidé par l'EMA et le SGA. Les responsables de segment et le directeur général du numérique et des systèmes d'information et de communication, la MOA du socle numérique ministériel mutualisé (DIRISI) et l'agence du numérique de défense (AND) sont membres de droit de ce comité de pilotage.

3.2. **Les instances de gouvernance thématique**

Des instances de gouvernance spécialisées s'ajoutent aux instances de gouvernance générales pour apporter une vision thématique des systèmes d'information et de communication de la défense et proposer les arbitrages nécessaires, le cas échéant. Elles concernent notamment :

- la gouvernance des fréquences ;
- la gouvernance de l'urbanisation (volet fonctionnel) et de l'architecture technique et applicative du SIC de la défense ;
- la gouvernance des données ;
- la gouvernance de la sécurité du numérique.

Ainsi, pour assurer la cohérence d'ensemble du système d'information et de communication de la défense, le directeur général du numérique et des systèmes d'information et de communication est assisté par les instances ministérielles spécialisées suivantes :

- la commission ministérielle des fréquences de la défense, qui prend en compte les aspects opérationnels et techniques ;
- la commission ministérielle d'urbanisation et le sous-comité de cohérence des architectures (SC²A) ;
- la commission ministérielle des données.

Les instances ministérielles spécialisées comprennent des représentants des membres du conseil du numérique et des systèmes d'information et de communication et les responsables des états-majors, directions ou services concernés.

Elles se réunissent sur convocation de leur(s) président(s), qui fixe(nt) l'ordre du jour des réunions, ou à la demande de l'un de leurs membres.

3.2.1. La gouvernance des fréquences

Déclinée de l'article 12 du décret de référence 1), la gouvernance des fréquences est détaillée dans l'instruction de référence 15).

La chaine ministérielle des fréquences et des positions spectro-orbitales est placée sous l'autorité du directeur général du numérique et des SIC qui s'appuie pour son pilotage sur l'Officier général chargé des fréquences de la Défense.

La gouvernance des fréquences s'exerce ainsi dans les domaines suivants :

- orientation des projets et programmes d'armement dès le stade des études de faisabilité ;
- évolutions des réglementations nationales, européennes et internationales ;
- gestion du spectre et des positions orbitales au profit des organismes du ministère ;
- protection juridique des installations radioélectriques d'infrastructure ;
- contrôle de l'emploi du spectre et lutte contre les brouillages subis ;
- emploi du brouillage par les armées.

La gouvernance des fréquences repose sur la commission ministérielle des fréquences (CMF), coprésidée par le directeur général du numérique et des systèmes d'information et de communication et par le chef d'état-major des armées ou son représentant, selon les termes de l'instruction de référence 15).

Organe de concertation, de décision, d'information et de retour d'expérience, elle adresse les problématiques et propositions relatives aux fréquences vers le comité exécutif du conseil du numérique et des systèmes d'information et de communication (CECNUM).

Se réunissant au moins une fois par an, elle associe les états-majors d'armée, les grands commandements et directions, ainsi que les directeurs des organismes directement rattachés au ministre. Elle peut également solliciter des experts, internes ou externes au ministère, en fonction des sujets traités.

La DGNUM en assure le secrétariat permanent.

3.2.2. La gouvernance de l'urbanisation et de l'architecture technique et applicative

3.2.2.1. Urbanisation (volet fonctionnel)

L'urbanisation permet aux autorités d'assurer la gouvernance du système d'information en alignant le SIC de la défense sur la stratégie retenue par le ministère. L'organisation et la rationalisation du SIC de la défense selon une approche fonctionnelle sont matérialisées au plus haut niveau par un plan d'occupation des sols (POS[19]), en lien avec le cadre commun d'urbanisation du SI de l'État.

La gouvernance d'urbanisation s'appuie sur la commission ministérielle d'urbanisation, instance de concertation, de décision, d'information et de retour d'expérience pour tous les sujets liés à la rationalisation fonctionnelle et à l'urbanisation des SIC.

La commission ministérielle d'urbanisation est présidée par le directeur général du numérique et des systèmes d'information et de communication. Elle se réunit au moins deux fois par an. Elle rassemble l'ensemble des responsables de zones fonctionnelles (RZF), ainsi que les autorités de domaines et les responsables de segment.

La commission ministérielle d'urbanisation s'appuie sur les travaux permanents du comité ministériel d'urbanisation animés par la DSI Groupe. Ce comité peut être saisi par tout acteur du numérique.

La commission ministérielle d'urbanisation porte les principales missions suivantes :

- elle instruit les pistes de rationalisation qui lui sont proposées par le comité ministériel d'urbanisation ;
- elle s'assure du rattachement de chaque projet au secteur le plus pertinent du POS et procède, le cas échéant, aux arbitrages qui lui sont soumis ;
- elle étudie et arbitre, le cas échéant, les demandes d'évolutions du POS présentées par le comité ministériel d'urbanisation qui a préalablement conduit les travaux de concertation requis avec les acteurs du numérique concernés. In fine, elle valide le POS et en assure la diffusion.

3.2.2.2. Architectures technique et applicative

La gouvernance des architectures technique et applicative s'appuie sur le sous-comité de cohérence des architectures (SC²A) pour valider les architectures des systèmes d'information du ministère.

Rattaché fonctionnellement au comité exécutif du conseil du numérique et des systèmes d'information et de communication (CECNUM), le SC²A est placé sous la

responsabilité du DGNUM et se réunit en tant que de besoin. Le SC²A délivre un avis formel pour valider les architectures d'un nouveau système d'information ou pour toute évolution majeure ou lors du renouvellement de son homologation. Il examine également les demandes de recours à des hébergements informatiques externes au ministère des armées. Le cas échéant, les réserves et recommandations formulées dans l'avis devront faire l'objet d'un suivi par le projet et d'une nouvelle présentation devant le SC²A.

Le SC²A est constitué par des architectes SIC représentant les différents organismes qui concourent à l'architecture d'entreprise du système d'information et de communication du ministère. Sa composition regroupe l'ensemble des compétences techniques permettant d'instruire les questions relatives aux systèmes d'information, aux réseaux de télécommunications et à leur sécurité incluant leur défendabilité.

Le CEMA, le DGA et le SGA en sont membres de droit.

3.2.3. La gouvernance des données

La gouvernance des données organise toutes les décisions relatives aux données au sein du ministère en matière d'inventaire, de stockage, de production, de circulation, d'exploitation, de conservation, de diffusion et de protection des données.

Le cadre stratégique de la gouvernance ministérielle des données, les principes directeurs et la définition des rôles et responsabilités sont fixés par la politique ministérielle des données[20].

La gouvernance ministérielle des données s'appuie sur les principaux acteurs suivants :

- le DGNUM en tant qu'administrateur ministériel des données, des algorithmes et des codes sources (AMDAC) ;
- le directeur des données (D2) au niveau de chacun des grands subordonnés. Ce rôle peut être décliné dans les états-majors, directions et services sous le rôle de directeurs des données délégués (D3). Les organismes rattachés directement au ministre désignent également un directeur des données ;
- l'administrateur des données de zone fonctionnelle (ADD-ZF) désigné par le RZF. Pour sa zone fonctionnelle, il est responsable de la description des métadonnées standardisées incluant les règles de gestion et de qualité des données, ainsi que de la cohérence des données de référence.

Les données à caractère personnel relevant du RGPD sont traitées par les fonctions suivantes[21] :

- le directeur des affaires juridiques en tant que délégué à la protection des données (DPD) ministériel. Le DPD du ministère n'a pas de compétence sur les établissements publics ou sous tutelle qui sont tenus de désigner leur propre DPD ;
- le responsable de traitement désigné selon une logique organique au sein des organismes relevant directement du ministre, au sein des organismes relevant du périmètre CEMA, DGA et SGA.

La gouvernance des données s'appuie sur les instances suivantes :

- la commission ministérielle des données (CMD), instance de concertation, de décision, d'information et de retour d'expérience, pour tous les sujets liés à la gouvernance des données.
  Présidée par le DGNUM, la CMD se réunit au moins une fois tous les deux mois, et en tant que de besoin. Le DPD est associé à la CMD. Elle adresse les problématiques et propositions relatives aux données vers le CECNUM.
- une comitologie subsidiaire définie par le DGNUM en tant qu'AMDAC dans un document de politique ministérielle des données.

3.2.4. La gouvernance de la sécurité du numérique

L'organisation et la gouvernance de la sécurité du numérique au sein du ministère des armées sont définis dans des textes spécifiques relatifs à la protection des installations, moyens et activités de la défense.

4. EXAMEN DES PROJETS ET SYSTÈMES

4.1. **Articulation avec la gouvernance capacitaire**

Le numérique et le capacitaire entretiennent des interactions fortes.

Tout ce qui relève du segment SIOC porte, *a priori*, des enjeux capacitaires et est examiné par la gouvernance capacitaire. L'EMA définit les modalités pratiques d'examen des dimensions DORESE[22] des SIOC. Certaines opérations d'investissement du domaine numérique peuvent être conduites comme des opérations d'armement, régies par l'instruction ministérielle de référence 14). S'agissant du socle numérique ministériel mutualisé, les autres segments sont associés à cette gouvernance.

Hors SIOC, de nombreuses opérations d'investissement du domaine capacitaire portent des enjeux relevant de la gouvernance numérique. Il s'agit notamment des composantes de systèmes d'armes relatives à la préparation de mission, la restitution de mission, l'analyse, l'exploitation et la capitalisation de données de masse, la restitution technique pour la logistique intégrée, la formation assistée par ordinateur, la simulation d'entrainement. Il s'agit également des interfaces avec le socle numérique ministériel en particulier les réseaux, l'hébergement et les passerelles. Il s'agit enfin des enjeux fréquentiels pour les télécommunications et les radars.

Les instances de gouvernance numérique peuvent donc être amenées à traiter d'orientations et prescriptions ayant des impacts sur les opérations d'armement du domaine numérique ou non (gouvernance des données, fréquences, urbanisation des SIOC, sécurité du numérique…). La bonne prise en compte de ces prescriptions par une opération d'armement est vérifiée au travers des instances décrites dans les instructions de références 13) et 14), notamment par la participation de la direction générale du numérique et des systèmes d'information et de communication à ces instances.

4.2. **Modalités d'examen des projets et systèmes**

Le sous-chapitre 4.2 concerne les opérations SIC au sens de l'instruction ministérielle de référence 16).

4.2.1 Principes généraux

L'objectif est d'assurer une gouvernance harmonisée pour les projets et SIC en service du ministère.

Les responsables de segment [décrits dans l'arrêté de référence 7)] sont responsables du changement des phases (préparation, réalisation, utilisation) décrites dans l'instruction ministérielle de référence 16).

Ils s'appuient pour cela sur des jalons dont le nombre et le degré d'approfondissement sont adaptés selon la nature du projet ou de l'évolution majeure du système considérés et dont les livrables sont fournis par l'autorité cliente, qui bénéficie, le cas échéant, du soutien de nombreux acteurs comme le (ou les) RZF, l'autorité de domaine et la DSI Domaine concernée, le (ou les) directeur(s) des données concerné(s).

Pour les projets et SI en service relevant des ZF de son périmètre et confiés à une DSI sur laquelle il a autorité, le responsable du segment est responsable de tous les changements de phases et des franchissements de jalons.

Dès lors que le projet ou l'évolution majeure considérée est confié à une DSI Domaine ne relevant pas de son autorité, le responsable du segment délègue la responsabilité et la présidence des changements de phases et des franchissements de jalons au grand subordonné dont relève la DSI désignée. Celui-ci associera le responsable de la zone fonctionnelle concernée et rendra compte de ses actions dans les instances de gouvernance du segment.

D'une manière générale, tout projet de SIC doit :

- être inscrit dans le portefeuille d'une DSI Domaine. La maîtrise d'ouvrage déléguée (MOAd) peut être confiée soit à la DSI Domaine ou soit à l'AND ;
- répondre à un besoin fonctionnel, exprimé par une autorité cliente ;
- être confié à une équipe projet et disposer de ressources humaines et financières ;
- être appréhendé sous l'angle du cycle de vie du produit, afin d'anticiper notamment les questions de soutien, d'évolutivité, d'archivage et de retrait de service ;
- respecter les cadres énoncés par la DSI Groupe ;
- s'inscrire dans la gouvernance ministérielle des données (description des métadonnées, ouverture, consommation et/ou production de référentiels de données, qualité, diffusion) ;
- être conforme aux exigences réglementaires, en particulier en matière de protection des données à caractère personnel et de protection du secret ;
- prendre en compte les enjeux de sécurité du numérique ;
- prendre en compte les enjeux fréquentiels éventuels (droit d'utilisation du spectre compte tenu des autres utilisateurs notamment).

4.2.2. Définition / déroulement des jalons

Les phases préparation, réalisation et utilisation sont initiées et clôturées par un jalon décisionnel.

Préparation – Étude préalable

Le jalon initial de la phase de préparation est appelé **jalon 0 (J0)**.

Sur la base de l'expression de besoin initial (EBI) ou d'une évolution majeure du système, le franchissement du J0 peut être prononcé. Il marque l'autorisation formelle de mener une étude de faisabilité (technique, management du projet et impacts organisationnels…) afin de fixer le périmètre, d'identifier les options possibles (développement spécifique, achats sur étagère, modernisation d'un système existant…).

Un calendrier général du projet est proposé.

Un responsable de conduite de projet (RCP) est désigné sous couvert de l'autorité de domaine et en accord avec la DSI concernée.

L'expression de besoin initial (EBI) ou d'une évolution majeure du système et l'étude de faisabilité constituent le dossier de lancement (DL).

Sur la base du DL, et après examen par la CEI dans le cas des projets inscrits sur la liste annuelle des opérations d'investissement (LOI), le responsable du segment compétent prononce la décision de clôturer l'étape « étude préalable » autorisant le passage à l'étape suivante « spécification » lors du jalon 1.

Le franchissement du **jalon 1 (J1)** marque l'autorisation de lancement de tout projet ou évolution majeure.

Préparation - Spécification

L'autorité cliente est responsable de l'étape « spécification » qui permet notamment de rédiger les spécifications générales, d'identifier les grandes fonctions (analyse fonctionnelle), en tenant compte des différents cadres, dans le respect du triptyque coûts, délais, performances.

Le cas échéant, un démonstrateur ou POC[23] peut être réalisé pour lever certaines incertitudes des futurs utilisateurs. Le plan de développement associé identifiera alors la stratégie de PMV[24] à mettre en œuvre en phase de réalisation.

Le cas échéant, une stratégie d'interface peut être nécessaire.

Un dossier de spécification (DS) adapté à la complexité du projet est fourni. Le DS est alors instruit par l'autorité cliente et présenté au responsable de segment.

La conduite du changement et le soutien logistique intégré (SLI[25]) doivent être anticipés.

Pour les projets identifiés à fort enjeu ministériel ou dont le montant prévisionnel global est supérieur ou égal à 5 millions d'euros, un dossier doit être soumis pour avis conforme au DGNUM[26]. Ceci concerne les projets se situant au stade du lancement des études de conception ou du cahier des charges fonctionnel, ou du cahier des clauses techniques particulières (CCTP). Pour les projets soumis au contrôle préalable de la CEI, l'examen du dossier en CEI vaut soumission au titre de l'avis conforme DGNUM.

Pour les projets relevant du SI de l'État[27] et dont le montant prévisionnel global est supérieur ou égal à 9 millions d'euros, un dossier doit être soumis pour avis conforme au DINUM[28], via le DGNUM. Pour les projets soumis à l'avis conforme DINUM, il n'est pas nécessaire de soumettre un dossier au titre de l'avis conforme DGNUM.

Ces avis conformes DGNUM ou DINUM sont nécessaires pour autoriser le changement de phase.

L'ensemble des documents produits constitue le dossier de réalisation initial (DR_0). Le DR_0 comprend l'ensemble des éléments listés au § 3.3 - *Clôture de la phase de préparation* de l'instruction de référence 16), notamment le périmètre du projet, son calendrier prévisionnel et le devis estimatif associé.

Sur la base du DR_0, le responsable du segment compétent, prononce la décision de clôturer la phase de préparation et d'entrer dans la phase de réalisation lors du jalon 2.

Le franchissement du **jalon 2 (J2)** permet à l'autorité compétente de prononcer le changement de phase.

Réalisation

La démarche d'acquisition ou de développement interne définie permet, le cas échéant, le lancement des procédures d'achat requises ou les contrats de service nécessaires. L'aboutissement de cette procédure de contractualisation permet de mettre à jour le dossier de réalisation initial DR_0 pour constituer le dossier de réalisation final DR_1, comprenant notamment le périmètre du projet, son calendrier et le devis de référence associé.

Sur la base du DR_1, et après examen par la CEI dans le cas des projets inscrits sur la liste annuelle des opérations d'investissement (LOI), le responsable du segment compétent prononce le franchissement du **jalon 3 (J3)** qui marque le lancement des travaux de réalisation.

La phase de réalisation se poursuit avec les activités suivantes : notification du ou des contrats, début des prestations, développement / paramétrage, finalisation des modalités techniques d'hébergement et de déploiement (sur l'internet ou le socle du ministère), finalisation des modalités de formation, d'accompagnement au changement, de mise en service et de soutien tant matériel que logiciel, opérations de vérification - vérification d'aptitude (VA) et vérification de service régulier (VSR).

L'ensemble des documents nécessaires à la mise en exploitation d'une première version opérationnelle constitue le dossier d'utilisation (DU).

Sur la base du DU, le responsable de segment prononce le franchissement du **jalon 4 (J4)** marquant l'entrée dans la phase d'utilisation.

Utilisation

Le franchissement du **jalon 5 (J5)** marquant la mise en service opérationnelle de la version couvrant l'ensemble des fonctionnalités fait l'objet d'une décision du responsable de segment ou de son délégataire.

L'utilisation de l'application par les utilisateurs se poursuit jusqu'à son décommissionnement.

Le retrait de service d'un système d'information s'inscrit dans une démarche de maitrise du patrimoine applicatif et doit être anticipé. À cette fin, les responsables de segment identifient, via les responsables SIC des organismes et les informations contenues dans SICL@DE, les systèmes dont la fin de vie prévisionnelle est inférieure à deux ans, afin d'en anticiper tous les impacts.

Après consultation des ADS utilisatrices de ces systèmes, l'autorité cliente établit, avec le service historique de la défense (SHD), le dossier de retrait de service (DRS) et le soumet à l'avis du responsable de la zone fonctionnelle concernée. La commission *ad hoc* statue alors sur le décommissionnement des applications lors d'un jalon 6 (J6). Le franchissement du **jalon 6 (J6)** marque la décision autorisant le décommissionnement. Le décommissionnement sera effectué par l'hébergeur de l'application.

Le sort réservé aux données générées par le SI est défini dans la stratégie d'archivage élaborée avec le soutien du SHD (dès la phase de préparation du projet) et entretenue durant toute la vie du système.

5. PUBLICATION

La présente instruction est publiée au *Bulletin officiel des armées*.

Le ministre des armées,

Sébastien LECORNU.

Notes

[1] Le système d'information et de communication de la défense est constitué de l'ensemble organisé des ressources permettant de collecter, traiter, transmettre et stocker les données sous format numérique qui concourent aux missions du ministère, à l'exception des ressources mises en oeuvre par la direction générale de la sécurité extérieure.
[2] Comité ministériel d'investissement.
[3] Commission d'examen des investissements.
[4] DPID : direction de la protection des installations, moyens et activités de la défense.
[5] SIOC : systèmes d'information opérationnels et de communication ; SIST : systèmes d'information scientifiques et techniques ; SIAG : systèmes d'information, d'administration et de gestion.
[6] DSI : Direction des systèmes d'information.
[7] RZF : responsable de zone fonctionnelle ; RQF : responsable de quartier fonctionnel.
[8] DGNUM : direction générale du numérique et des systèmes d'information et de communication.
[9] COMCYBER : commandement de la cyberdéfense.
[10] AQSSI : autorité qualifiée sécurité des systèmes d'information, définie dans l'instruction de référence 10).
[11] L'architecture d'entreprise est une démarche visant à aligner avec la stratégie d'entreprise l'ensemble des couches de l'entreprise (métier, fonctionnelle, applicative et technique). L'architecture d'entreprise comprend l'urbanisation et l'architecture technique.
[12] FSSI : fonctionnaire de sécurité des systèmes d'information.
[13] Le périmètre du « socle numérique ministériel mutualisé » est défini à l'article 5. 4° de l'arrêté de référence 7).
[14] DIRISI : direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense.
[15] COF : comité d'orientation fonctionnel.
[16] Responsable SIC : son rôle principal est d'être le coordonnateur des besoins opérationnels et le garant de la cohérence des SIC utilisés relevant du portefeuille de la DSI Domaine à laquelle il appartient.
[17] RSE : responsabilité sociétale des entreprises.
[18] Cf. arrêté de référence 7) portant création et organisation d'instances relatives au SIC de la défense.
[19] Le plan d'occupation des sols (POS) est un cadre de représentation synthétique et structurée de la vision fonctionnelle, applicative et informationnelle (données) du système d'information. Il est constitué de secteurs subdivisés dont les principaux sont :
- la Zone Fonctionnelle (ZF) qui représente un découpage fonctionnel du système d'information ;
- le Quartier Fonctionnel (QF), subdivision d'une ZF, qui est lié à la nature de l'information traitée.
[20] Cf. note n° 117/ARM/DGNUM/DG/NP du 5 avril 2022 relative à la diffusion de la politique ministérielle des données.
[21] Instruction RGPD du 31 janvier 2020 de référence 18).
[22] DORESE pour Doctrine, Organisation, Ressources, Équipement, Soutien spécifique, Entrainement.
[23] POC : Proof Of Concept, ou preuve de concept.
[24] PMV : Produit minimum viable.
[25] Le SLI comprend notamment le MCO (maintien en condition opérationnelle), le MCS (maintien en condition de sécurité, l'appui aux utilisateurs, la formation.
[26] Se référer à l'arrêté de référence 3).
[27] SI de l'État : tous les SIAG à l'exception de ceux qui font intervenir, nécessitent ou comportent des supports ou informations classifiés.
[28] Se référer à l'arrêté de référence 4).

ANNEXES

ANNEXE 1.
TEXTES DE RÉFÉRENCE.

Références :

1) Décret N° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication (JO n° 148 du 29 juin 2018, texte n° 13) ;

2) Décret N° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique (JO n° 251 du 27 octobre 2019, texte n° 2) ;

3) Arrêté du 28 juin 2018 pris pour l'application de l'article 5 du décret N° 2018-532 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication (JO n° 148 du 29 juin 2018, texte n° 16) ;

4) Arrêté du 5 juin 2020 pris pour l'application de l'article 3 du décret N° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique (JO n° 182 du 26 juillet 2020, texte n° 1) ;

5) Arrêté du 23 avril 2021 portant création de l'agence du numérique de défense (JO n° 104 du 4 mai 2021, texte n° 4) ;

6) Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale (JO n° 185 du 11 août 2021, texte n° 1) ;

7) Arrêté ARM/SGA/DAJ/D2P/BDOD du 9 septembre 2022 portant création et organisation d'instances relatives au système d'information et de communication de la défense ;

8) Circulaire N° 6264/SG du 27 avril 2021 relative à la politique publique de la donnée, des algorithmes et des codes sources (n.i. BO);

9) Instruction ministérielle N°1544/DEF/CAB/-- du 17 janvier 2017, version du 10 août 2020 relative à la défense-sécurité des activités, moyens et installations relevant du ministre de la défense (n.i. BO) ;

10) Instruction ministérielle N° 7326/ARM/CAB du 25 juin 2018, portant sur la politique de sécurité des systèmes d'information du ministère de la défense (PSSI-M) (n.i. BO);

11) Instruction ministérielle N° 101000/ARM/CAB du 24 décembre 2018 relative à la politique de lutte informatique défensive du ministère des armées ;

12) Instruction ministérielle N° 210214/ARM/SGA/DRH-MD du 18 juillet 2019 relative à l'organisation, à la gouvernance et aux processus de la fonction ressources humaines au sein du ministère des armées ;

13) Instruction N° 100/ARM/CAB du 15 février 2019 relative aux opérations d'investissement du ministère des armées ;

14) Instruction N° 1618/ARM/CAB du 15 février 2019 sur le déroulement des opérations d'armement ;

15) Instruction N° 3/ARM/DGNUM/NP du 19 avril 2019 portant sur la gouvernance ministérielle des fréquences et des positions orbitales (n.i. BO) ;

16) Instruction N° 2476/ARM/CAB/CC6 du 29 avril 2019 portant sur la conduite des projets de système d'information et de communication ;

17) Instruction N° 31416/ARM/CAB du 22 juillet 2019 relative aux attributions et au fonctionnement de la commission d'examen des investissements (n.i. BO) ;

18) Instruction N° ARM/SGA/DAJ/DPSP du 31 janvier 2020 relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense ;

19) Instruction N° 2067/ARM/CAB/CC6 du 7 mai 2020 relative à l'innovation de défense au sein du ministère des armées ;

20) Instruction N° 13259/ARM/DGA/AND/D du 16 juin 2021 relative aux missions et à l'organisation de l'agence du numérique de défense ;

21) Instruction ministérielle N° 7326-2/DEF/CAB du 21 juillet 2021. Volet technique de la politique de sécurité des systèmes d'information du ministère de la défense (PSSIM-T) (n.i. BO).

ANNEXE 2.
DESCRIPTION DES DIX-SEPT DOMAINES DE L'ÉCOSYSTEME NUMÉRIQUE ET SIC DU MINISTÈRE.

Armée de Terre - Préparation des forces :

Le domaine Armée de Terre – préparation des forces regroupe les systèmes d'information concourant aux missions opérationnelles de l'armée de terre, au recrutement, la formation et la gestion de son personnel, à sa communication institutionnelle, à sa vie courante ainsi qu'à la gestion des données qui les alimentent.

MCO Terrestre :

Le domaine MCO Terrestre regroupe les métiers qui permettent de conduire la réparation des matériels aéroterrestres et de gérer les biens et stocks associés. Il couvre aussi tous les métiers qui participent directement à la réalisation des missions de la DC SIMMT.

Marine - Préparation des forces :

Le domaine Marine – préparation des forces regroupe les systèmes d'information concourant aux missions opérationnelles de la Marine, en mer et à quai, au recrutement et à la formation de son personnel ainsi qu'à la gestion des données qui les alimentent.

MCO Naval :

Le domaine MCO Naval regroupe les systèmes d'information qui permettent d'assurer la disponibilité technique des navires, embarcations et équipements du milieu naval des 3 armées et la gestion des stocks correspondants.

Armée de l'Air et de l'Espace - Préparation des forces :

Le domaine Armée de l'Air et de l'Espace – préparation des forces regroupe les systèmes d'information concourant aux missions opérationnelles de l'Armée de l'Air et de l'Espace, le domaine spatial, le recrutement et à la formation de son personnel, ainsi qu'à la gestion des données qui les alimentent.

MCO Aéronautique :

Le domaine MCO Aéronautique regroupe les systèmes d'information qui concourent au maintien en condition d'emploi des matériels aéronautiques (aéronefs, centres de commandement, radars sol, radio sol-air, matériels d'environnement, équipement du personnel navigant, …) des armées et la gestion des stocks correspondants.

Commandement et Contrôle et Interarmées (C2&IA) :

Le domaine Commandement et Contrôle (C2) et Interarmées regroupe les systèmes d'information opérés par les Organismes interarmées sous l'autorité du CEMA. Ce domaine englobe les systèmes de C2, les opérations spéciales, les munitions, l'énergie opérationnelle, la formation, la doctrine et le soutien interarmées, l'acheminement stratégique, la codification des matériels, la météo et la géographie militaires, et la sécurité aéronautique.

Renseignement :

Le domaine Renseignement regroupe l'ensemble des systèmes d'information concourant à la captation technique, à l'orientation, au traitement, à l'exploitation et la diffusion du Renseignement d'Intérêt Militaire (RIM). Il n'inclut cependant pas les systèmes techniques de Renseignement propres à chaque armée.

Appui SIC :

Le domaine Appui SIC regroupe les systèmes d'information concourant au fonctionnement de la DIRISI, notamment en tant qu'opérateur et acheteur SIC ministériels. Cela comprend la numérisation de son offre de services, les applications de gestion des biens et de gestion des stocks nécessaires à la logistique des équipements SIC, les SI d'exploitation à l'exclusion des SI intégrés dans le socle numérique.

Soutien Commissariat des armées :

Le domaine Soutien Commissariat des armées regroupe l'ensemble des SI qui concourent aux 11 fonctions du soutien : habillement et équipements commissariat, alimentation et restauration, hébergement et hôtellerie, gestion de site et soutien multiservices, soutien à la condition du personnel, transport routier individuel et collectif, administration du personnel militaire et solde, soutien à la mobilité professionnelle, acquisition de biens et services courants aux forces armées, exécution financière des forces armées, conseil juridique aux forces et contentieux. Ce domaine impose une prise en compte essentielle de la cybersécurité du fait de ses nombreuses interactions extérieures.

Soutien Santé :

Le domaine Soutien Santé regroupe l'ensemble des SI concourant à la mission du SSA, articulés autour de 4 fonctions : soigner, ravitailler, former, chercher. Le domaine Soutien Santé inclut la mise en œuvre et l'exploitation du réseau Intrasan qui dessert principalement les hôpitaux d'instruction des armées.

Systèmes numériques de l'armement :

Le domaine recouvre l'ensemble des métiers de la DGA en support de ses missions majeures qui sont de préparer le futur des systèmes de défense, équiper les forces armées de façon souveraine, promouvoir la coopération européenne, soutenir les exportations d'armement. Son périmètre fonctionnel comprend l'ensemble des activités des domaines de performances de la DGA, y compris les activités d'expertises, essais et expérimentations conduits par la DGA.

Ressources Humaines (RH) :

Le domaine RH recouvre les métiers relatifs au périmètre fonctionnel suivant : condition du personnel, droits financiers, effectifs et masse salariale, formation, gestion individuelle et collective, pourvoi des postes.

Immobilier :

Le domaine immobilier couvre les métiers de la gestion du patrimoine immobilier du MINARM, du logement, de l'énergie et de l'environnement.

Finances Achats :

Le domaine "Finances Achats" recouvre l'ensemble des métiers suivants :

- "Finances" [Comptabilités (analytique, budgétaire, générale), Contrôle et Audit internes financiers, Dépenses, Élaboration et programmation budgétaire, audit interne comptable et financier, Gestion des actifs hors immobilier, Gestion financière de projets, Pilotage budgétaire et comptable, Plafond d'emploi et masse salariale, Recettes non fiscales, Dialogue institutionnel sur les lois de finances] ;
- "Achat Public" [Passation et exécution des marchés, Gestion Relation Client, Opérateurs économiques, Gouvernance des achats].

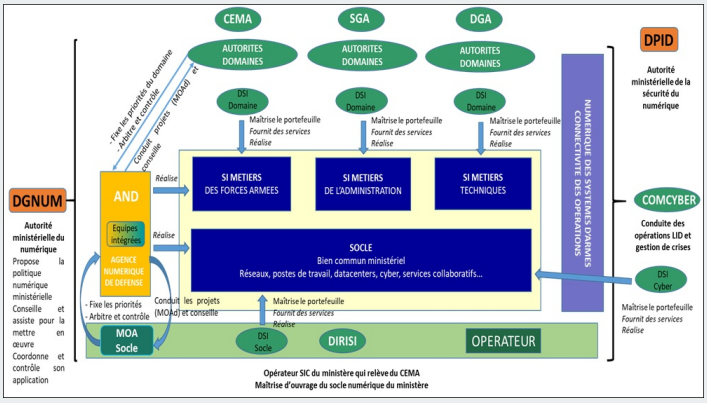
Transverse :

Le domaine Transverse recouvre les métiers du SGA non couverts par les domaines RH, Immobilier, Finances Achats et Renseignement de sécurité et de défense.

Renseignement de sécurité et de défense :

Ce domaine recouvre l'activité de renseignement dans le domaine du terrorisme, de l'espionnage, de la subversion, du crime organisé à l'encontre du ministère et de la base industrielle et technologique de défense (BITD). Le renseignement produit sert à ce que les entités puissent se protéger au bon niveau, tant sur le domaine physique qu'immatériel. La protection concerne les personnels, les installations, les informations visés par les adversaires de contre ingérence.

ANNEXE 3.
REPRÉSENTATION SIMPLIFIÉE DES RELATIONS ENTRE LES DIFFÉRENTS ACTEURS.



ANNEXE 4.
LE CYCLE DE VIE D'UN PROJET.